Patent Claims

1. A method for the protected transmission of data words, involving

- provision of a first data word (X1),

- transformation of the first data word (X1) into a sequence comprising at least one second data word (X2) by a first transformation rule (T1),

- transformation of at least one of the second data words (X2) into a third data word (X3) by a second transformation rule (T2), and

- checking whether a prescribed relationship exists between the third data word (X3) and a comparison data word (VX).

2. The method as claimed in claim 1, wherein an alarm function (ALARM) is executed if the prescribed relationship does not exist between the third data word (X3) and the comparison data word (VX).

3. The method as claimed in claim 1 or 2, wherein before the second data word (X2) is transformed it is modified such that a distinct relationship exists between the third data word (X3) and the comparison data word (VX).

4. The method as claimed in claim 3, wherein the modification of the second data word (X2) involves adding information (I).

5. The method as claimed in claim 1 or 2, wherein a distinct relationship exists between the third data word (X3) and the comparison data word (VX).

6. The method as claimed in one of claims 1 to 5,

wherein the distinct relationship is the identity of the third data word (X3) to the comparison data word (VX).

7. The method as claimed in one of claims 1 to 6, wherein the first data word (X1) is the comparison data word (VX).

8. The method as claimed in one of claims 1 to 7, wherein the second transformation rule (T2) is a reverse depiction of the first transformation rule (T1).

9. The method as claimed in one of claims 1 to 6, wherein the first data word (X1) is transformed to produce the comparison data word (VX) by a third transformation rule (T3).

10. The method as claimed in claim 9, wherein the result of the third transformation rule (T3) applied to the first data word (X1) is in the prescribed relationship with the result of the application of the second transformation rule (T2) after the first transformation rule (T1) to the first data word (X1).

11. The method as claimed in claim 9 or 10, wherein the second transformation rule (T2) is the identity and the first and third transformation rules (T1, T3) are the same.

12. A circuit arrangement for the protected transmission of data words, having

- a data input which is connected to a first transformation device (DEC) which transforms a first data word (X1), which is applied to the data input, into a sequence (S2) of data words which comprises at least one second data word (X2),

- a second transformation device (R1) which is coupled to the first transformation device (DEC) and which transforms at least one of the second data words (X2) into a third data word (X3),

- a checking device (COMP) which has the third data word (X3) and a comparison data word (VX) supplied to it and which checks whether the third data word (X3) and the comparison data word (VX) are in a prescribed relationship.

13. The circuit arrangement as claimed in claim 12, wherein it performs an alarm function (ALARM) if the third data word (X3) and the comparison data word (VX) are not in the prescribed relationship.

14. The circuit arrangement as claimed in either of claims 12 and 13, wherein the first data word (X1) is supplied to the checking device (COMP) as comparison data word (VX).

15. The circuit arrangement as claimed in one of claims 12 to 14, wherein a device is provided which modifies the second data word (X2) such that the prescribed relationship between the comparison data word (VX) and the third data word (X3) is distinct.

16. The circuit arrangement as claimed in one of claims 12 to 14, wherein the first transformation device (DEC) modifies the second data word (X2) such that the prescribed relationship between the comparison data word (VX) and the third data word (X3) is distinct.

17. The circuit arrangement as claimed in one of claims 12 to 16, wherein a third transformation device (R2) is provided which is connected upstream of the

checking device (COMP) and which transforms the first data word (X1) applied to the input into the comparison data word (VX).

18. The circuit arrangement as claimed in claim 17, wherein the second transformation device (R1) is in a form such that the third data word (X3) matches the second data word (X2).

19. The circuit arrangement as claimed in claim 17, wherein the first and third transformation devices (DEC, R2) execute the same transformation.

20. The circuit arrangement as claimed in one of claims 12 to 19, wherein the prescribed relationship is the identity of the comparison data word (VX) and the third data word (X3).

21. The circuit arrangement as claimed in one of claims 12 to 20, wherein the first transformation device (DEC) is arranged between an arithmetic and logic unit (CPU) and a memory device (MEM).

22. The circuit arrangement as claimed in one of claims 12 to 21, wherein the first transformation device (DEC) has at least one further transformation device connected upstream and/or downstream of it.